SECURITY ASSESSMENT
STANDARDS AND PROCEDURES

Release Date 17 November 2000

FEDSIM Project Number 20164EDE-01

Prepared by:

FEDERAL SYSTEMS INTEGRATION MANAGEMENT CENTER
OFFICE OF INFORMATION TECHNOLOGY INTEGRATION

Prepared for:

THE DEPARTMENT OF EDUCATION
STUDENT FINANCIAL ASSISTANCE ORGANIZATION

FOREWORD

The Office of Information Technology Integration (OITI) would like to thank those involved in the development of this document.

Bob Padgett
Paul Jackson
Laura McConnell
Jack Norrell
Philip Norton
Bruce Wilner

EXECUTIVE SUMMARY

This document has been prepared for the Department of Education, Student Financial Assistance Organization (SFA). SFA has embarked upon an ambitious program to provide state-of-the-art information access to its user population: students, financial institutions, and financial professionals at learning institutions.

Due to the extensive user demographics as well as the visibility of the program, SFA decided to impose the rigors of Independent Verification and Validation (IV&V) upon critical application developments. As a pioneer Performance Based Organization, SFA desired to establish standards and criteria with which to measure the performance of its IV&V agents. Therefore, it directed the preparation of standards and procedures for:

- IV&V conduct
- Security Assessment
- IV&V Reporting
- IV&V Performance Measures

Each of these standards and procedures documents is being prepared as a separate volume. Once finalized, they will be combined into an IV&V Handbook.

The purpose of this document is to establish standards and procedures for assessing the information security of designated SFA systems under development. The standards and procedures are to reflect the best practices of security engineering and management and are to be applicable to each of the system models in use at SFA.

TABLE OF CONTENTS

Page

4.1 INTRODUCTION

4.2 SECURITY ASSESSMENT STANDARDS

4.3 SECURITY ASSESSMENT PROCEDURES

TABLE OF CONTENTS (Cont'd)

4. SECURITY ASSESSMENT STANDARDS AND PROCEDURES

4.1 Introduction

This introductory section establishes the purpose and scope of these standards and procedures.

4.1.1 Scope

These standards and procedures (S&P) are to be applied during the security assessment (SA) of SFA systems.

They are to guide and control the activities of Independent Verification and Validation (IV&V) Teams. Therefore, they do not address security assessment activities inappropriate to IV&V or performed by other organizations. For example, penetration testing is not included herein.

Only systems in development or upgrade are to be targets of SA. Thus, these S&P do not necessarily reflect assessment of deployed systems.

All Target Systems (i.e., the subjects of the security assessments) shall be Major Applications as defined by OMB Circular A-130, Appendix III, “Security of Federal Automated System Resources.”

4.1.2 Assumptions

It is assumed that the SA Team (SAT) will have access to development artifacts (documentation, code, tests, etc.) and staff in order to conduct the SA. The specific items can be gleaned from the standards and procedures contained herein.

It is assumed that the SAT will be engaged sufficiently early in the IPT Development Process (i.e., prior to the Systems Requirements Analysis Phase) so that a full SA can be performed. Otherwise, a *limited scope* SA will be negotiated and documented in the SA charter.

4.1.3 Tailoring

These S&P may be tailored for the specific target system. Tailoring will be based upon two factors:

- The target system model

- The degree of security risk

In general those standards tagged as A-130 requirements should not be altered or deleted. If that is unavoidable, then authorization should be obtained from the Department of Education or SFA Security Manager.

For SA with special security considerations, additional standards and procedures may be required. These should be documented in the Security Assessment Plan.

Tailoring is discussed further in Section 4.3 - Security Assessment Procedures.

4.1.4 Performance-Based Features

In support of SFA's mission to become the first U.S. Government Performance Based Organization (PBO), these SA standards have been formatted to *measure* the quality of the developer's system security program. The security assessor can either enter a checkmark in the first column (see the sample table below) or can enter a numerical score. The checkmark indicates the existence of conformance to the standard while the numerical score is a judgment of the *degree* to which the standard has been met. The table also contains columns for the relative weight of each standard (*Quality Value*) and for a *weighted score*. If weighted scoring is to be used, then the SAT must establish the weight values in advance and obtain concurrence from the SFA IV&V Program Manager.

The security requirements listed in this document are derived from the standards and guidelines shown in columns 3 through 7 of the table below. The presence of an 'X' indicates that the requirement is called out by the standard at the top of the column. A full reference for each of these documents is given in the bibliography.

Score	ASSESSMENT REQUIREMENT	A-130 Appendix III	NIST 800-18	ED IT Security Policy	ISO 17799	EASI SWDS Sec 3	Quality Value	Weighted Score	Note
5	A security plan is written and published.	X	X	X			10	50	(1)
6	Security policies (rules of behavior) are documented.	X	X	X	X	X	9	54	(2)

Notes:

(1) The security plan for the xyz project is written but not yet published.

(2) Some key Rules of Behavior were not included. The SAT considers these to be critical to the xyz risk management.

4.2 Security Assessment Standards

This major section lists all of the SA standards. After a subsection covering general items, the standards are grouped into Management Controls, Operational Controls, and Technical Controls.

4.2.1 General

General standards include the composition of and charter for the SAT as well as those related to profiling the target system. The latter topic is vital since it focuses the SA on the system vulnerabilities and is used to tailor the standards and procedures.

4.2.1.1 Security Assessment Team

The SAT shall have a charter describing the purpose, scope, critical success factors and ground rules for the assessment/inspection.

Each key SA Team member should meet the Information Systems Audit and Control Association (ISACA) standards for Information Systems Control Professionals. If this is not feasible, then key team members should possess current security credentials (e.g., a valid security clearance issued by a U.S. Government agency).

Each SA Team member shall execute a non-disclosure agreement against release or use of any private, sensitive, or proprietary information encountered during the SA.

4.2.1.2 Target System Profile

<u>Identification</u>

The target system should be identified both by name, version number, and release date. If more than one version is to be assessed, all versions should be noted.

<u>Responsibility</u>

The organizations and individuals responsible for target system security should be documented in the assessment report. Their roles may include development, operation, administration, or other functions.

<u>Description</u>

The SAT shall review the description of the target system, its overall architecture, and its special functional and/or technical features. Normally, this information is provided by the program office developing the system in its business case.

Interconnections/Interfaces

One key area is the sharing of the target system information with external systems. Therefore, all interconnections should be well understood by the SAT and documented in the initial assessment report.

System Model

The system model describes how information is input, stored, and output. It defines how users interact with information, e.g., via a Web interface. It also describes the high-level development strategy, e.g., heavy use of Commercial Off-the-Shelf (COTS) software vice custom programming. The system model is key to tailoring Technical Control Requirements.

Information Protection Profile

The development organization should have defined the information that must be protected in terms of its requirements for Confidentiality, Integrity, and Availability. If not, this task must be accomplished by the SAT because it forms the basis for assessment of the effectiveness of controls.

4.2.2 Management Controls

The security controls included in this category focus on the management of the computer security system and the management of risk. The section begins with a discussion of risk assessment and management. Following that, the management control standards are listed in four subsections:

- Security Review Policy
- Rules of Behavior
- Life Cycle Security Policies
- Authorize Processing

4.2.2.1 Risk Assessment and Management

While there are various system models within the SFA enterprise, the most severe challenge to security is presented by systems meeting the following description:

> *Highly interactive systems performing secure transactions involving back-end data while connected to a public network (the Internet)*

To set the stage for the SA standards and procedures, it is useful to review the threats to be countered. The information in this section is not intended to be part of the standards or procedures. However, a security assessment must determine whether an appropriately rigorous threat analysis has been performed.

Threat Analysis

Threat Analysis attempts to identify the categories of threat agents, the mechanisms available to them, their motives, possible actions and the potential impact on the enterprise. The basic axiom of threat analysis is:

> *Threat agents (with motives) take actions using mechanisms to exploit vulnerabilities to cause an impact against a target.*

The following views of the threat environment provide a structure for performing threat analysis.

Threat Agent

Threats to information systems normally originate from humans. Analyzing threat agents involves categorizing individuals that interact with the system. For example, at the highest level, SFA users can be grouped into Students, Financial Organizations, and Schools. In addition, there is the SFA and VDC staff that administers and maintains the system. Each of these groups should be further analyzed if subgroups could present a unique set of threats. For example, students that are merely inquiring about financial assistance represent a potential threat quite different from students that possess loans.

It is important to note that humans can interact intentionally or unintentionally. Therefore, threats can be accidental as well as deliberate. Also, it should be noted that threats don't always originate with people. For example, when SFA systems rely on the safeguards of external systems, then there is the threat that a failure in the external system could indirectly threaten SFA information assets.

Threat Mechanism

For each user type, the mechanisms available should be analyzed. Mechanisms normally fall into one of the following categories:

- Physical
- Electronic
- Operational
- Environmental

Threat Motive

Again, for each user category, the possible motives should be identified. Although this might seem irrelevant, it is often useful in the design of specific countermeasures. Typical motives might include:

- Money
- Peer Pressure
- Anarchy
- Revenge
- Curiosity
- Self-Education
- One-Upmanship

Threat Action

The possible range of threat actions is too broad to list in this document. However, once agents, mechanisms and motives have been identified, then it is possible to compare these to the target system environment to define a set of potential threat actions. The most important aspect of this analysis is to keep in mind that the agent must have *opportunity* to conduct any action.

Threat Impact

Security assessment includes risk assessment. One component of risk assessment is the consideration of the *consequences* of a realized risk. For example, if the consequence is insignificant, then risk abatement resources might be better applied elsewhere. Analyzing the potential impacts of threats is essential in establishing risk consequence.

Impact analysis should consider the following as a minimum:

- Damage or destruction
- Disclosure
- Unauthorized release of information
- Denial of service
- Modification or tampering

- Fraud, waste and abuse
- Information theft
- Intellectual property rights
- Privacy
- Financial information
- Passwords/identification
- Use as an attack vehicle
- Data corruption (unintentional)

Probability

Risk Assessment should consider not only the potential consequences of the threat action, but also the likelihood of its occurrence. For example, even the most devastating impacts might not warrant risk reduction expenditures if the probability of its happening is on the order of 10^{-9} (one in one billion). On the other hand, even the least impact must be eliminated if it occurs with sufficient frequency.

There are several techniques for estimating probability, such as the well-accepted Delphi method. The SAT should select one that is appropriate for the program and describe the method briefly in the assessment plan.

Risk Estimation

There are a number of acceptable methods for estimating risk from the components of threats and probability. A moderately quantitative approach is described in Appendix B – Risk Factor Calculation.

4.2.2.2 Security Review Policy

The SAT shall assess the target system program for the presence of the following:

Score	ASSESSMENT REQUIREMENT	A-130 Appendix III	NIST 800-18	ED IT Security Policy	ISO 17799	EASI SWDS Sec 3	Quality Value	Weighted Score	Note
	There is a written policy calling for an independent review of the security controls at least every three years.	X	X	X	X	X			
	Reviews provide verification that the controls selected afford a level of protection commensurate with the acceptable level of risk for the system.		X	X					
	Reviews determine whether controls have become outdated due to technological advances, changing threats, and/or personnel change.		X	X	X	X			

4.2.2.3 Rules of Behavior

One aspect of management control of security is the establishment of a set of rules by which users access the information. The SAT shall assess this rule set for the following qualities:

Score	ASSESSMENT REQUIREMENT	A-130 Appendix III	NIST 800-18	ED IT Security Policy	ISO 17799	EASI SWDS Sec 3	Quality Value	Weighted Score	Note
	A set of rules of behavior has been established in writing for each system.	X	X	X	X				
	The rules are determined by the acceptable level of risk.	X	X	X					
	The rules of behavior clearly delineate responsibilities and expected behavior of all individuals with access to the system.	X	X	X					
	The Rules cover work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of government equipment, the assignment and limitation of system privileges, and individual accountability.		X						

Score	ASSESSMENT REQUIREMENT								
	Rules of Behavior are made available to every user prior to receiving authorization for access to the system.		X	X					
	The security required by the rules is only as stringent as necessary to provide adequate security for information in the system.	X	X	X					
	Rules include appropriate limits on interconnections to other systems.	X	X						
	Users are required to sign statements that they understand the rules of behavior.	X	X		X				

4.2.2.4 Authorization to Process

The phrase "Authorization to Process" means the permission granted by a management official (e.g., the Chief Information Officer (CIO)) for a system to process live information. Sometimes, this is referred to as accreditation. The SAT's report may provide one input to the authorization decision.

Score	ASSESSMENT REQUIREMENT	A130 Appendix III	NIST 800-18	ED IT Security Policy	ISO 17799	EASI SWDS Sec 3	Quality Value	Weighted Score	Note
	There is a policy and process for authorization of processing prior to live operation.	X	X	X	X				
	Re-authorization is required whenever there is a significant change to the system but at least every three years.	X	X	X					
	The security assessment, risk assessment, and other required reviews/audits have been satisfactorily completed.		X						

4.2.3 Operational Controls

This section describes those security mechanisms that are normally implemented and executed by people as opposed to automated systems components. It contains the subsections:

- Personnel Security

- Physical and Environmental Protection

- Transport of Production Data
- Contingency Planning
- Application Software Maintenance Controls
- Data Integrity/Validation Controls
- Documentation
- Security Awareness and Training
- Incident Response Capability

4.2.3.1 Personnel Security

Section 4.2.2.3, Rules of Behavior, listed standards for managing personnel in the area of systems security. This section focuses upon the policies for the control of personnel access to sensitive information.

Score	ASSESSMENT REQUIREMENT	A-130 Appendix III	NIST 800-18	ED IT Security Policy	ISO 17799	EASI SWDS Sec 3	Quality Value	Weighted Score	Note
	Individuals who are allowed to bypass significant technical and operational security controls are screened.	X	X	X	X				
	Screening occurs prior to authorization for such access and periodically thereafter.	X	X	X					
	Personnel control policies are documented.			X		X			
	All positions have been reviewed for sensitivity level.		X	X					
	Security-critical functions are divided among different individuals in such a way as to ensure that no one individual has all necessary authority or information access which could result in fraudulent activity.		X	X					

4.2.3.2 Physical and Environmental Protection

The assessment of physical security is applicable to the SFA office areas and the Virtual Data Center (VDC).

Score	ASSESSMENT REQUIREMENT	A-130 Appendix III	NIST 800-18	ED IT Security Policy	ISO 17799	EASI SWDS Sec 3	Quality Value	Weighted Score	Note
	The facility in which sensitive equipment and information is located has controls restricting the entry and exit of personnel and media.	X	X	X	X	X			
	An effective fire detection and suppression capability is present.		X	X	X	X			
	There has been an evaluation of the effects of a failure in public utilities (power, HVAC, water, sewage) on system operation and a plan for recovery.		X	X		X			
	There has been an evaluation of the effects of building structural failure and plumbing/sprinkler leaks together with a plan for recovery.		X			X			
	The threat of data interception has been considered and countered as appropriate. This includes interception by direct observation, by data transmission, and by electromagnetic means.	X	X	X	X	X			
	The organization has an effective policy and procedure for protecting information stored on portable computers.	X	X	X		X			
	There is a clearly defined security perimeter which segregates other tenants in multi-tenant buildings.				X	X			
	The perimeter of a building or site is physically sound (i.e., solid walls and doors with bars, alarms, locks, etc.).			X	X	X			
	A manned reception area or other means to control physical access to the space is in place.				X	X			
	Visitors are supervised or cleared, their date and time of entry and departure recorded.				X	X			
	Employees are required to wear visible identification badges.				X	X			
	Access rights to secure areas are regularly reviewed and updated.	X			X	X			
	Backup equipment and media are located remotely from the main site.			X	X				
	Suitable intruder detection systems are installed and regularly tested.				X	X			

Score	ASSESSMENT REQUIREMENT								
	Third party support services personnel are granted access to secure areas only when required. This access should be authorized and monitored.			X	X				
	Uninterruptable power supplies (UPS) are employed to support orderly close down of equipment.				X				
	Backup generators are used if the system must continue to operate through power outages.				X				
	Power and telecommunications cabling carrying data or supporting information services is protected from interception or damage.				X				
	All major equipment is inventoried with model number, serial number, location and responsible person/organization recorded.					X			
	There are documented procedures for control of pass keys and access cards for all employees, contractors, cleaning staff, and security personnel.	X		X		X			
	Controls must exist for disposal of all sensitive material.	X			X	X			

4.2.3.3 Transport of Production Data

This section lists standards for assessing the control of sensitive information in a form that could be transported out of the primary computing facility. It does not address transmission of information over a network.

Score	ASSESSMENT REQUIREMENT	A130 Appendix III	NIST 800-18	ED IT Security Policy	ISO 17799	EASI SWDS Sec 3	Quality Value	Weighted Score	Note
	There is a procedure to ensure that only authorized individuals can read, copy, alter or remove printed or electronic material.		X	X	X				
	There is a procedure to ensure that only authorized individuals pick up, receive, or deliver sensitive input and output material.		X						
	There are audit trails for receipt of sensitive materials.		X						

Score	ASSESSMENT REQUIREMENT								
	There is a policy and procedure for labeling sensitive material when in physical form.		X	X					
	There are procedures for storage, handling, and destruction of sensitive material.		X	X					
	Printed reports policies must be documented.					X			

4.2.3.4 Contingency Planning

This section addresses one of the main security goals – continuance of business operations following an impacting event. Recovery from security breaches, natural disasters, or inadvertent damage can be handled by a common plan.

The SAT should look for the following qualities in the organization's business continuity plan.

Score	ASSESSMENT REQUIREMENT	A-130 Appendix III	NIST 800-18	ED IT Security Policy	ISO 17799	EASI SWDS Sec 3	Quality Value	Weighted Score	Note
	Documented contingency plans are in place to permit continued mission critical functions following a catastrophic event.	X	X	X	X				
	Contingency plans have been tested.	X	X	X	X				
	Contingency plans meet the requirements of FIPS Publication 87, Guidelines for ADP Contingency Planning		X						
	The plans make clear the conditions for their activation including how to assess the situation.				X				
	The plans include, as appropriate, public relations management and effective liaison with public authorities (e.g., police, fire department, etc.).				X				
	The plans detail fallback procedures which describe the actions to be taken to move essential business activities or support services to alternative temporary locations, and to bring business activities back into operation in the required time frames.				X				
	The plans include resumption procedures which describe the actions to be taken to return to normal business operations.				X				

Score	ASSESSMENT REQUIREMENT								
	The plans include a maintenance schedule which specifies how and when the plan will be tested and the process for maintaining the plan.				X				
	The plans address training of those personnel involved in the backup and recovery process.				X				

4.2.3.5 Application Software Maintenance Controls

These standards are for the control of changes to the target system's applications software. The goal is to ensure that changes are controlled and that a complete record of changes is maintained.

Score	ASSESSMENT REQUIREMENT	A-130 Appendix III	NIST 800-18	ED IT Security Policy	ISO 17799	EASI SWDS Sec 3	Quality Value	Weighted Score	Note
	There is a written procedure for changing and testing updates to the COTS software before putting it into production.	X	X		X				
	Periodic audits of users' computers are conducted to ensure that only legal, licensed software is installed.	X	X		X				
	There is a clear record of ownership of the software.	X	X						
	There is a mechanism for controlling changes to the software and for reviewing them against security standards.	X	X	X	X				
	The change control process calls for testing all changes and for authorizing release.	X	X		X				
	A full record is maintained of all milestone events in the change process.	X	X		X				
	All commercial software is copyrighted or otherwise has an established ancestory (i.e., is not shareware).	X	X						
	The system should include a test facility to enable administrators to test security changes before placing them into production.					X			

Score	ASSESSMENT REQUIREMENT								Note
	All security changes are tested fully before being placed into production including security testing of password files, privilege definition tables, encryption algorithms and sensitive application data sets.					X			
	All newly procured software is isolated and tested prior to use.					X			
	Software received is verified against the software suppliers or distributors installation checklist					X			
	Software is checked for viruses using a proprietary tool.			X		X			
	Executable programs are write-protected and/or encrypted to prevent modification.					X			
	There are routine comparisons of programs to secure authorized versions.					X			
	Checksum routines are used for verification of programs.					X			
	Periodic checks are made to ensure that virus detection (and other security) software programs have not been automatically deactivated (e.g., due to license expiration).				X				

4.2.3.6 Data Integrity/Validation Controls

The purpose of these controls is to prevent loss, modification, or misuse of user data in application systems. Data integrity controls protect information from accidental or malicious alteration or destruction. The term "Validation controls" refers to tests and evaluations used to determine compliance with security specifications and requirements.

Score	ASSESSMENT REQUIREMENT	A-130 Appendix III	NIST 800-18	ED IT Security Policy	ISO 17799	EASI SWDS Sec 3	Quality Value	Weighted Score	Note
	Software is installed for the detection and elimination of viruses		X	X	X				
	Virus scanning occurs at network login, diskette insertion, or downloads from untrusted sources.		X	X					
	There are procedures for updating virus signature files.		X						

Score	ASSESSMENT REQUIREMENT								
	Anti-Virus solutions protect not only individual hosts on a network but also networks against hostile applets and network threats.					X			
	Users are prohibited from installing unauthorized software on any internal computer.			X		X			
	Program and data files are backed up regularly.			X		X			
	The system uses reconciliation routines (i.e., checksums, record counts, hash totals) to detect discrepancies in user data.		X		X				
	The system uses integrity verification programs that check data consistency and reasonableness, validate data during input and processing, etc.		X		X				
	Intrusion detection software should be used.		X						
	System performance is automatically monitored in real time to detect any availability problems.		X						
	Message authentication is used to ensure that the sender of a message is known and that the message has not been altered during transmission.		X						
	Controls are in place to ensure that application programs are run at the proper time and order.				X				
	Controls are in place to ensure that outputs are validated.				X				

4.2.3.7 Documentation

Documentation is included as a security control because it explains the workings of the system including the security mechanisms.

Score	ASSESSMENT REQUIREMENT	A-130 Appendix III	NIST 800-18	ED IT Security Policy	ISO 17799	EASI SWDS Sec 3	Quality Value	Weighted Score	Note
	The system documentation formalizes security and operational procedures specific to the system.		X						
	There is a written policy for the control of system operations documentation.					X			
	System documentation is stored securely.				X				

Score	ASSESSMENT REQUIREMENT								
	The access list for system documentation is kept to a minimum and authorized by the application owner.				X				
	System documentation held on a public network, or supplied via a public network, is appropriately protected.				X				

4.2.3.8 Security Awareness and Training

Since users have security responsibilities, they must be properly instructed before accessing the target system. Users of public access systems (e.g., Web-based applications) should be constrained by the security features of the application itself. Notification of security control may be made at the time of the user's access.

The SAT shall assess the security awareness and training program for the following:

Score	ASSESSMENT REQUIREMENT	A130 Appendix III	NIST 800-18	ED IT Security Policy	ISO 17799	EASI SWDS Sec 3	Quality Value	Weighted Score	Note
	A security awareness and training program has been established.	X	X	X	X				
	The program addresses each system user according to their access authorization and security responsibilities.		X	X	X				
	Training is conducted before access is permitted.				X				
	Training includes how to respond to security incidents and malfunctions				X				

4.2.3.9 Incidence Response Capability

The objective of this capability is to minimize the damage from security incidents and malfunctions and to monitor and learn from such incidents.

Score	ASSESSMENT REQUIREMENT	A130 Appendix III	NIST 800-18	ED IT Security Policy	ISO 17799	EASI SWDS Sec 3	Quality Value	Weighted Score	Note
	There is a formal incidence response capability.	X	X	X	X				
	There is a means of informing users of the procedures for reporting the different types of incidents (security breach, threat, weakness, or malfunction).	X	X	X	X				
	There are explicit procedures for recognizing and handling incidents (i.e., what files and logs should be kept, who to contact, etc.).			X					
	There are mechanisms in place to record the types and volumes of incidents and malfunctions and to quantify the costs.				X				

4.2.4 Technical Controls

Technical controls are those mechanisms that are executed by the computer system itself. This section contains the standards for assessing those controls. The standards have been grouped by the purposes of the controls:

- User identification and authentication
- Authorization
- Public Access
- Audit Trails and Logs

The final subsection discusses those special controls that are specific to the target system model.

4.2.4.1 Identification and Authentication

Unauthorized people and processes can be prevented from entering the target system via well-chosen identification and authentication mechanisms. Therefore, this area is “ground zero” for the security assessment. It is essential that users be clearly and unambiguously identified and authenticated, for that is the only way to establish user accountability.

Score	ASSESSMENT REQUIREMENT	A-130 Appendix III	NIST 800-18	ED IT Security Policy	ISO 17799	EASI SWDS Sec 3	Quality Value	Weighted Score	Note
	The identification mechanism ensures that a unique identity is assigned to each user.		X	X	X	X			
	The identification mechanism is able to correlate each action to the user.		X	X					
	The system enables the organization to ensure that all user identifications belong to *currently* authorized users.		X	X		X			
	User accounts that are inactive for an extended time are automatically disabled.		X		X	X			
	Policy sets (and software enforces) the minimum and maximum password length.		X	X	X	X			
	Policy sets (and software enforces) the allowable character set for passwords.		X	X		X			
	Policy sets (and software enforces) the maximum age for a password and the mechanism for forcing refreshment.		X	X	X	X			
	Policy sets (and software enforces) the number of generations of expired passwords that are not eligible for re-use.		X	X		X			
	Policy sets (and software enables) procedures for changing passwords.		X	X		X			
	Policy sets (and software enables) procedures for handling lost and compromised passwords.		X	X	X	X			
	If biometric controls are used, there is a clear description of how the controls are to be implemented.		X						
	If token controls are used, there is a clear description of how the controls are to be implemented (e.g., PINs, one-time passwords, challenge-response protocol, etc.).		X						
	The level of enforcement of the access control mechanism (network, operating system, or application) is defined.		X						
	The system encrypts passwords for transmission and storage.		X	X	X	X			
	If feasible, passwords should be automatically generated.		X						
	The system checks new password candidates against the list of disallowed passwords.		X	X	X	X			

Score	ASSESSMENT REQUIREMENT								
	The system takes action (e.g., notifies the security administrator, disables the user account, etc.) whenever a pre-defined number of invalid access attempts have occurred for a given user identifier within a pre-defined time limit.		X		X	X			
	The system supports verification that all default passwords have been changed.		X		X	X			
	Scripts with embedded passwords are prohibited.		X		X	X			
	Passwords are stored separately from application software.				X				
	Passwords are not displayed on the user's screen.			X	X	X			
	Policies and mechanisms for single signon are described in writing together with compensating controls.		X						
	If digital signatures are used, the technology conforms to FIPS 186, Digital Signature Standard and FIPS 180-1, Secure Hash Standard.		X			X			
	The use of electronic signatures is fully documented together with the security controls provided.		X						
	The system supports cryptographic key management including key generation, distribution, storage, entry, use, destruction, and archiving.		X						
	The identification mechanism used is able to integrate with other security applications.					X			
	The identification code is not associated with other commonly used numbers or identifiers, such as social security numbers, savings, checking, loan or other financial account numbers, PINs or the customer's mother's maiden name.					X			
	The identification codes are issued securely to prevent compromise of PINs default passwords, tokens or smart cards.					X			
	Access to the password file or database is restricted to authorized processes.					X			
	Passwords are stored as shadow passwords (i.e., the password storage file should not be readable).					X			

Score	ASSESSMENT REQUIREMENT								
	The electronic tokens are usable from all the access points available to the user in question.					X			
	There is a specified policy for managing electronic tokens as part of enterprise-wide security policy. This includes issuing, validating and disabling electronic tokens.					X			
	There is a guaranteed specified maximum time from the report of a lost or stolen electronic token to the time that it is disabled.					X			
	Electronic or cards used as one-time password generators must have a specified time cycle of password expiry (e.g., 60 seconds).					X			
	The passwords generated by one-time password generation electronic tokens or cards must be unique.					X			
	An authorized Certificate Authority shall manage all digital certificates.					X			
	The biometric devices used are able to support all relevant types of users.					X			
	The biometric identifier is unique for each user.					X			
	The biometric identifier is a permanent characteristic of the user.					X			
	Authentication of users (by name and password) over the Web is performed via a secure connection based on a protocol such as SSL or SHTTP					X			
	Usernames and passwords are not distributed in the same communication (e.g., e-mail or fax communication).					X			
	User accounts are restricted from performing multiple concurrent logins using the same user login and password.					X			

4.2.4.2 Logical Access Controls (Authorization)

NIST 800-18 defines logical access controls to be those "system-based mechanisms used to specify who or what (e.g., in the case of a process) is to have access to a specific resource and the type of access that is permitted."

This major subsection lists those controls that authorize or restrict the activities of users and systems personnel *within the application*. The SAT should assess each control as applicable both to the sensitivity of the information as well as to the technology employed for storing and accessing it.

Score	ASSESSMENT REQUIREMENT	A-130 Appendix III	NIST 800-18	ED IT Security Policy	ISO 17799	EASI SWDS Sec 3	Quality Value	Weighted Score	Note
	There is a formal policy that divides users into access classes with clearly defined access authority.	X	X	X	X	X			
	Access control recognizes that users' access privileges change over time or as the result of a specific event.	X	X		X	X			
	There is a formal, written policy that defines the authority granted to each user or class of users.		X	X					
	This policy adheres to the philosophy of "least privilege".		X	X	X				
	There are procedures for granting new users access and for changing access privileges when the user changes to a new class.		X		X				
	Authorization policies separate user privileges such that no one individual has all of the authority and/or access to commit fraud without collusion.		X	X					
	The target application includes an Access Control List (ACL) that maps users or user classes to the types of access permitted.		X						
	The application owner is able to restrict access rights of other users, administrators, and operators to the application programs, data, and files.		X	X					
	There is a process for reviewing and updating the ACL.		X						
	There are mechanisms to detect unauthorized access attempts.			X		X			
	If policy permits users to delegate access permissions or make copies of files available to other users, then there is a written procedure for how and under what circumstances this may be done.		X	X					
	If encryption is used to prevent unauthorized access to sensitive files, then it adheres to FIPS Pub 46-2.		X						
	Authorization mechanisms are able to map the system wide user access rights to mechanisms in individual application software and operating systems.					X			
	Resources such as data files, programs, application systems and sensitive media are explicitly defined to the security software.					X			

Score	ASSESSMENT REQUIREMENT								
	It is possible to assign access rights for all resources in the system to individual users as well as all users in a group, according to a stated policy.					X			
	Once authorized, users will have definite access time windows within which they can access applications.					X			
	Security firewalls are used to prevent access to systems from unauthorized hosts.			X		X			
	There are adequate access controls over critical system resources including system libraries, system catalogues and directories, program libraries (source, object, executable), data dictionaries, log files, job control statement libraries.					X			
	System security related profiles and other security resources are accessible to authorized security personnel exclusively.					X			
	System security related functionality in the system is accessible only to authorized security personnel.					X			
	There are adequate controls over available functions that could be used to bypass system security.					X			

4.2.4.3 Public Access Controls

If the public accesses the target system, then the SAT should assess the following controls:

Score	ASSESSMENT REQUIREMENT	A-130 Appendix III	NIST 800-18	ED IT Security Policy	ISO 17799	EASI SWDS Sec 3	Quality Value	Weighted Score	Note
	There are controls to prevent public users from modifying information inappropriately.	X	X	X	X				
	Copies of information for public access are placed on a separate system.	X	X		X				

Score	ASSESSMENT REQUIREMENT								
	Storage of on-line information for access by the public is kept separate from "live" data.		X						
	Information for distribution is kept on CD ROM if possible.		X						
	The public is never be allowed access to "live" databases.		X						
	Information distributed to the public is scanned for viruses.		X						
	There is a formal authorization process before information is made available to the public via the target system (e.g., Web site).			X	X				
	Digital signatures are used to protect software, data, and other information requiring a high level of integrity.		X		X				
	There is a security mechanism to protect all vulnerable access points in the enterprise network.					X			
	There are no single points of failure among vulnerable resources in the system.					X			
	There is a mechanism to enforce strong authentication for users accessing systems remotely. The remote authentication mechanisms include dial-back modems and one-time passwords.			X		X			
	A firewall shall protect the entry point for a remote access node.					X			
	Sensitive information transmitted over the Web is encrypted.					X			
	The Server and Client both authenticate themselves in case of sensitive information being transmitted.					X			
	A filter or a firewall is used to restrict traffic from the Web server host to the internal network.			X		X			
	Source routing is turned off at the router so that the Web server host cannot be used to forward packets to hosts in the internal network.					X			
	Public servers are placed on subnets separate from internal networks.					X			
	Network routers are configured to restrict traffic from public servers to internal networks.					X			

Score	ASSESSMENT REQUIREMENT								
	Authoritative (genuine and correct) copies of the contents of Web site information are kept on a host separate from and more secure than the Web server host.					X			
	Network servers are configured to offer only essential services. This is to ensure that other services cannot be used to attack the host and impair or remove desired network services.					X			
	All Web servers connected to the Internet will have a firewall between the Web server and internal department networks.			X		X			
	Any internal Web servers supporting critical applications are protected by internal firewalls. Sensitive, confidential, and private information is never stored on an external Web server.					X			
	Web sites comply with federal government and SFA Web site hosting standards, policies and guidelines.					X			
	A link to the SFA standard privacy policy statement shall be placed on the initial ("splash") page of all SFA Websites.					X			
	If possible, firewalls are configured to block the reception of applets; from external sources and block the distribution of applets outside of internal networks unless authentication technology is used to protect it from untrusted sources.					X			
	A firewall is a part of a consistent overall organizational security architecture and supports the enterprise-wide security policy.			X		X			
	A firewall is able to accommodate new services and needs.					X			
	The firewall does not accept or allow new services until a security review of the proposed services is completed and results verified. This will ensure no risks are incurred that will threaten the firewall or the network behind it.			X					
	A firewall is able to deny all services except those specifically permitted.					X			
	The firewall host machine is protected by allowing only limited access to itself.					X			
	The firewall is able to support all standard authentication mechanisms.					X			

Score	ASSESSMENT REQUIREMENT								
	The firewall contains the ability to concentrate and filter dial-in access.					X			
	A firewall is able to restrict access to internal as well as external sites.					X			
	The firewall should contain mechanisms for logging traffic and suspicious activities.					X			
	The strength and correctness of the firewall is verifiable.					X			
	There are multiple points of failure for the firewall. (i.e., if one link in the network is compromised, the network is not open).					X			
	In case of remote access through dial-up lines, the firewall uses a secure technology like modem call-back.					X			

4.2.4.4 Audit Trails and Logs

These standards define the qualities that the SAT should look for in assessing the target system's security audit trail capability.

Score	ASSESSMENT REQUIREMENT	A-130 Appendix III	NIST 800-18	ED IT Security Policy	ISO 17799	EASI SWDS Sec 3	Quality Value	Weighted Score	Note
	The audit trail shall support accountability by providing a trace of user actions.	X	X	X					
	Access to online audit logs is strictly controlled.		X	X	X				
	The system shall provide an audit trail record for every logon.			X	X	X			
	The system shall provide an audit trail record for every attempt to read modify, add, create, or delete information.					X			
	The system shall provide an audit trail record for every attempted or successful database administrator/administration activities.					X			
	The system shall provide an audit trail record for every logging of authorized system access and resource usage.				X	X			
	The system shall provide an audit trail record for every logging of unauthorized access attempts				X	X			

Score	ASSESSMENT REQUIREMENT								
	The system shall provide an audit trail record for every logging of maintenance of security profiles or tables.					X			
	The system shall provide an audit trail record. for every logging of system environmental changes.				X	X			
	The system shall provide an audit trail record for every logging of privileged user activity.					X			
	The system shall provide an audit trail record for every logging of excessive access.					X			
	The system shall provide an audit trail record for every logging of use of sensitive commands.					X			
	For each recorded event, the audit record shall identify date and time of event.		X	X		X			
	For each recorded event, the audit record shall identify the user.		X	X	X	X			
	For each recorded event, the audit record shall identify type of event.		X	X		X			
	For each recorded event, the audit record shall identify success or failure of the event.			X		X			
	For each recorded event, the audit record shall identify name of the object being used or deleted.			X		X			
	The audit trail can be queried by user id, terminal id, application name, or date/time to create reports with selected information.		X						
	The system shall provide adequate retention of system log files.					X			
	The system shall provide maintenance of recovery logs.					X			
	The system shall limit the availability of functionality that can be used to override logging parameters.					X			
	All access to logs must be explicitly authorized.			X		X			
	All access violations must be formally reviewed and followed up by appropriate staff.					X			
	Privileged programs, users, or utilities may not bypass access restrictions.					X			
	Backups must be securely stored.					X			
	The system shall support log administration and monitoring activities including documented procedures for followup of serious security violations.					X			
	The system shall support production and review of security profile reports.					X			

Score	ASSESSMENT REQUIREMENT								
	The system shall support production and review of user activity reports.					X			
	The system shall provide support for regular IS management review of log of activities.					X			

4.2.4.5 System Model Specific Controls

This section defines technical controls with varying applicability depending on the target system model. For example, if the target system is to use encryption, then a (rather large) set of control qualities should be assessed by the SAT. Therefore, as part of the Security Assessment Plan, the SAT should select one or more of these control categories and further tailor the requirements listed in each category. The categories are:

- Single Sign-On
- Encryption and Public Key Infrastructure
- Directory Services
- Electronic Mail
- Electronic Data Interchange
- Database

Inasmuch as these controls are not *generally* applicable, the tables listing them have been included as Appendix C.

4.3 Security Assessment Procedures

This section defines the general procedures to be followed by the SAT in performing assessment of a target system. Inasmuch as the SAT is part of the larger SFA IV&V effort, these procedures have been synchronized with the corresponding IV&V tasks within the context of the SFA IPT development phases:

- System Requirements Analysis
- Preliminary System Design
- Detailed System Design

- Build and Test
- Integration Test
- Acceptance Test

In the sections below, the assessment procedures are mapped to those Section 4.2 standards that are appropriate to that phase.

The diversity of SFA projects is recognized. Therefore, as with the standards, it may be necessary to tailor these procedures as well. For example, the development might deviate from the IPT High-Level Process. When it is necessary to tailor these procedures, then the exact process should be documented in the SA Plan and concurrence requested from SFA management.

4.3.1 System Requirements Analysis Phase

It is assumed that SFA will not task the IV&V Team to begin the security assessment until after the Concept Design and Business Process Re-engineering Phases have concluded. However, should an earlier start be permitted, the activities in Section 4.3.1.1 should be started immediately.

4.3.1.1 General

The first step in the SA is the formation of the SAT and the establishment of the Security Assessment Plan. This brief plan should include the following:

- Identification of the target system
- Objective of the SA
- Scope of the SA
- Organization of the SAT
- Tailoring of the SA standards and procedures
- A schedule for the assessment

An important consideration when developing the SA Plan is to minimize impacts upon the development team. One effective way to accomplish this is to focus the assessment on recorded information (electronic or hardcopy) rather than on interviews and meetings. This has the added benefit of basing the assessment on “objective evidence” rather than on hearsay.

The next step is to conduct a brief analysis of the target system. This includes examination of the high-level architecture, concepts of operation, overall requirements, and processing environment. From this examination, it should be possible to categorize the system model, e.g., a Web application versus a back office batch system, etc.

Next, an analysis of the information contained within the system should be undertaken in order to identify categories requiring protection. This is referred to as a "protection profile." If the developer has already performed this analysis, then the SAT should review the results and supplement it as needed.

With this information in hand, the SAT is able to complete its two main preparatory tasks:

- Tailoring the standards to the system model and high-level security requirements

- Conducting the risk assessment in accordance with Section 4.2.2.1 (or validating the developer's risk assessment if available)

Finally, if the SAT has chosen to score the criteria in the standards tables (as opposed to using them strictly as a checklist) then the SAT members must assign weights to each criterion. Once completed, the checklists should be reproduced for each SAT member.

4.3.1.2 Security Requirements and Policy Assessment

During this phase of the development process, the SAT should perform assessment against the standards in the following sections:

Section 4.2.2.1 – Risk Assessment and Management
Section 4.2.2.2 – Security Review Policy
Section 4.2.2.3 – Rules of Behavior
Section 4.2.2.4 – Authorization to Process
Section 4.2.3.1 – Personnel Security

If information is not available for any particular item, but is expected later, then the SAT should note this on the checklist and schedule the assessment of those items for the phase in which they are expected.

Once all criteria have been checked, the SAT can compile its findings. If more than one member has scored the same set of criteria, then those scores must be reconciled. Then the team can prepare the SAT Report for System Requirements Analysis. The details of this report are specified in Section 5 (IV&V Reporting Standards and Procedures) of the SFA IV&V Handbook.

As part of the IV&V Team, the SAT will participate in the SFA IPT's System Requirements Review.

4.3.2 Preliminary System Design Phase

During this phase, the developer is evaluating various alternatives for technical security controls. Therefore, it may be premature to assess these controls. However, the security features of the physical facility should be known. If so, this phase presents an opportunity to assess the criteria contained in Section 4.2.3.2 – Physical Security and Environmental Protection.

If the target system is to be migrated to the VDC, then physical security assessment might not be necessary or appropriate. For example, if the VDC has been previously assessed, then a follow-on physical security assessment would only be necessary if the target system required changes that impacted the VDC security regimen.

As with the System Requirements Analysis phase, the SAT completes its activity in this phase with the preparation of the SAT Report for Preliminary System Design. Likewise, the SAT participates in Preliminary Design Review.

4.3.3 Detailed System Design Phase

Nominally, most of the SA will be concentrated in this phase, presuming that the developer has made most of the decisions relative to the security architecture. During this phase, the SAT should evaluate this architecture against the criteria contained in:

Section 4.2.3.3 – Transport of Production Data
Section 4.2.3.4 – Contingency Planning
Section 4.2.3.5 – Application Software Maintenance Controls
Section 4.2.3.6 – Data Integrity/Validation Controls
Section 4.2.4 – Technical Controls (all subsections)

It should be noted that the term “technical controls” includes all of the system model specific controls.

As before, the SAT will prepare the SAT Report, this time for the Detailed System Design. This report will be the most detailed since it reflects assessment of the lowest level security features of the target system. It will also contain an update of any issues raised by earlier reports.

It is crucial that all significant security issues existent at the end of the Detailed System Design phase be addressed expeditiously. To resolve them in a later phase will almost certainly impact the schedule and cost of the development.

This phase culminates in the Critical Design Review. The SAT will participate in this important milestone.

4.3.4 Build and Test Phase

During this phase, the SAT should follow up on any remaining security issues, perform continuing risk assessment, and assist in issue resolution/risk mitigation activities.

As appropriate, the SAT might also assess developer testing of security requirements at unit level.

The SAT Report for the Build and Test Phase will be an update of the reports previously submitted. Focus will be on open issues and risk mitigation.

The SAT will participate in Integration Test Readiness Review as part of the IV&V Team. If the developer has failed to satisfy any of the security-related entrance criteria, then the SAT should be prepared to present the status together with recommendations.

4.3.5 Integration Test Phase

The primary SAT activity in this phase is to assess developer testing of security requirements at the integration level. As part of the overall IV&V effort, system requirements will have been traced to integration tests. The SAT will examine this trace to determine which security-related requirements are to be verified during integration testing. For example, this test evolution will likely be the first opportunity to verify multi-application identification/authentication.

The SAT will report on the results of integration testing. This report might be a section of the overall IV&V report for integration testing or, if there are significant security requirements, a separate SAT report may be prepared.

The SAT will independently determine whether the developer has met the security-relevant entrance criteria for Acceptance Testing. The SAT should be prepared to present and discuss its recommendations at the Acceptance Test Readiness Review.

4.3.6 Acceptance Test Phase

The result of Acceptance Testing is a key input to the CIO's decision to deploy the target system. The developer should demonstrate that all security functionality is in place and working properly. The SAT will witness Acceptance Testing as part of the overall IV&V Team. As such, the SAT will focus upon the security-related requirements, but will also evaluate how overall system performance might impact on security. For example, each anomaly should be reviewed by the SAT to determine if it has security implications (including the proposed fix).

The SAT should review the disposition of all anomalies found during Acceptance Testing and witness the developer's regression testing following remedial actions.

In addition to test witnessing, the SAT may conduct independent testing of security requirements, as permitted by SFA. This testing must be on a "not to interfere" basis with the developer's testing. It should concentrate on areas where the developer testing is considered weak and on “off nominal” or stress conditions. Actual penetration testing is not the responsibility of the SAT.

During this phase, the SAT will also assess the target system against the standards contained in the following sections:

Section 4.2.3.7 – Documentation
Section 4.2.3.8 – Security Awareness and Training
Section 4.2.3.9 – Incidence Response Capability

The SAT Report for Acceptance Test should render a clear opinion of the target system performance in the area of security. It should address any open issues (including those from any of the previous phases) and present a clear recommendation for acceptance, conditional acceptance, or rejection of the system from the security perspective. This document may be part of the overall IV&V report for this phase or it may be a separate report.

The SAT will participate in Production Readiness Review. Any remaining security issues should be limited to management or operational controls. Any technical control issues should have been adjudicated in earlier phases.

If requested by SFA, the SAT should provide inputs to “lessons learned” exercises conducted during the Post Implementation Phase.

ACRONYMS

ACL	Access Control List
BSI	British Standards Institute
CIO	Chief Information Office
COTS	Commercial Off-The-Shelf
CRL	Certificate Revocation List
DAA	Designated Approving Authority
DES	Data Encryption Standard
EASI	Easy Access for Students and Institutions
EDI	Electronic Data Interchange
FIPS	Federal Information Processing Standard
GSS	General Support System
HTTP	Hypertext Transfer Protocol
ID	Identification
IP	Internet Protocol
IPR	In Process Review
IPT	Integrated Product Team
IR	Incident Report
ISACA	Information Systems Audit and Control Association
ISO	International Standards Organization
IT	Information Technology
IT	Integration Test
IV&V	Independent Verification & Validation
MIME	Multipurpose Internet Mail Extensions
MISPC	Minimum Interoperability Specification for PKI Components
NIST	National Institute of Standards and Technology
OSI	Open Systems Interconnect
PBO	Performance Based Organization
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure

ACRONYMS (Cont'd)

QA	Quality Assurance
SA	Security Assessment
S&P	Standards and Procedures
SAT	Security Assessment Team
SFA	Office of Student Financial Assistance
SHTTP	Secure HyperText Transport Protocol
SI&T	System Integration and Test
S/MIME	Secure MIME
SQL	Standard Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On
TRR	Test Readiness Review
UPS	Un-interruptable Power Supply

GLOSSARY

Acceptable Risk

Acceptable risk is a concern that is acceptable to responsible management, due to the cost and magnitude of implementing countermeasures.

Accreditation

Accreditation is the authorization and approval granted to a major application or general support system to process in an operational environment. It is made on the basis of a certification by designated technical personnel that the system meets pre-specified technical requirements for achieving adequate system security. See also Authorization to Process**,** Certification and Designated Approving Authority.

Authorization to Process

Authorization to process occurs when management authorizes a system based on an assessment of management, operational and technical controls. By authorizing processing in a system the management official accepts the risk associated with it. See also Accreditation, Certification, and Designated Approving Authority.

Availability Protection

Protection of system availability requires backup of system components and information, contingency plans, disaster recovery plans, and redundancy. Examples of systems and information requiring availability protection are time-share systems, mission-critical, time and attendance, financial, procurement, or life-critical applications.

Certification

Certification is synonymous with the phrase “authorization to process.” Certification is the technical evaluation that establishes the extent to which a computer system, application, or network design and implementation meet a pre-specified set of security requirements.

Confidentiality Protection

Protection of confidentiality requires access controls such as user ID/passwords, terminal identifiers, restrictions on actions like read, write, delete, etc. Examples of confidentiality-protected information are personnel, financial, proprietary, trade secrets, internal agency, investigations, other federal agency, national resources, national security, and high or new technology under Executive Order or Act of Congress.

GLOSSARY (Cont'd)

Designated Approving Authority (DAA)

The DAA is the senior management official who has the authority to authorize processing (accredit) an automated information system and accept the risk associated with the system.

Firewall

A firewall is a system (or network of systems) specially configured to control traffic between two networks. A firewall can range from a packet filter to multiple filters, dedicated proxy servers, logging computers, switches, hubs, routers and dedicated servers.

Gateway

A gateway is a secured computer system that provides access to certain applications. It cleans outgoing traffic, restricts incoming traffic and may also hide the internal configuration from the outside.

General Support System (GSS)

A GSS is an interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

Individual Accountability

Individual accountability requires individual users to be held responsible for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.

GLOSSARY (Cont'd)

Information Security

Information security is the preservation of confidentiality, integrity, and availability. Each of these attributes is defined as follows:

- Confidentiality – ensuring that information is accessible only to those authorized to have access

- Integrity – safeguarding the accuracy and completeness of information and processing methods

- Availability – ensuring that authorized users have access to information and associated assets when required

Major Application

A major application is a system that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

Networks

Networks include a communication capability that allows one user or system to connect to another user or system and can be part of a system or a separate system. Examples of networks include local area networks or wide area networks, including public networks such as the Internet.

Operational Controls

Operational controls address security mechanisms that are primarily executed by people (as opposed to systems).

Packet Filter

A packet filter stops or allows packets to flow between two networks according to predefined rules. A simple packet filter is a router. It works on the network layer of the Open Systems Interconnect (OSI) model.

Proxy

A proxy is a program which allows/disallows access to a particular application between networks. It works on the Application layer of the OSI model.

Risk

Risk is the possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.

Risk Assessment

Risk assessment is the structured analysis of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence.

Risk Management

Risk management is the ongoing process of assessing the risk to automated information resources. It is part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.

Rules of Behavior

These are the rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of federal government equipment, the assignment and limitation of system privileges, and individual accountability.

Sensitive Information

Sensitive information refers to information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under the Privacy Act, and information not releasable under the Freedom of Information Act.

GLOSSARY (Cont'd)

Sensitivity

Sensitivity in an information technology environment consists of the system, data, and applications that must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and availability. This level is determined by an evaluation of the sensitivity and criticality of the information processed, the relationship of the system to the organization's mission, and the economic value of the system components.

System

System is a generic term used for brevity to mean either a major application or a general support system.

System Operational Status

System operational status is either (a) Operational - system is currently in operation, (b) Under Development - system is currently under design, development, or implementation, or (c) Undergoing a Major Modification - system is currently undergoing a major conversion or transition.

Target System

The target system is the subject of the security assessment.

Technical Controls

Technical controls consist of hardware and software controls used to provide automated protection to the system or applications.

Threat

Threat is an activity, deliberate or unintentional, with the potential for causing harm to an automated information system or activity.

Vulnerability

Vulnerability is a flaw or weakness that may allow harm to occur to an automated information system or activity.

BIBLIOGRAPHY

British Standards Institute (BSI), "Information Security Management," British Standard BS 7799-1:1999. London, England: BSI, 1999.

Information Systems Audit and Control Association (ISACA), "Standards for Information Systems Control Professionals," www.isaca.org/standard/iscontrl.htm.

National Institute of Standards and Technology (NIST), "Computer Data Authentication," Federal Information Processing Standard (FIPS) Publication 113. Gaithersburg, MD: NIST, 1985.

NIST, "Data Encryption Standard (DES)," FIPS Publication 46-2. Gaithersburg, MD: NIST 1993.

NIST, "DES Modes of Operation," FIPS Publication 81. Gaithersburg, MD: NIST 1980.

NIST, "Digital Signature Standard (DSS)," FIPS Publication 186-1. Gaithersburg, MD: NIST 1998.

NIST, "Entity Authentication Using Public Key Cryptography," FIPS Publication 196. Gaithersburg, MD: NIST 1997.

NIST, "Guide for Developing Security Plans for Information Technology Systems," Special Publication 800-18. Gaithersburg, MD: NIST 1996.

NIST, "Secure Hash Standard," FIPS Publication 180-1. Gaithersburg, MD.

NIST, "Security Requirements for Cryptographic Modules," FIPS Publication 140-1. Gaithersburg, MD: NIST 1994.

NIST, "Password Usage," FIPS Publication 112 . Gaithersburg, MD: NIST 1985.

U.S. Office of Management and Budget (OMB), "Security of Federal Automated Information Resources," OMB Circular A-130, Appendix III. Washington, DC: OMB

U.S. Department of Education. "Project EASI/ED System-Wide Design Standards Document," 1999.

U.S. Department of Education. "SFA System Integration and Testing Approach, SFA Modernization," Undated.

Appendix B

RISK FACTOR CALCULATION

APPENDIX B. RISK FACTOR CALCULATION

Risk tends to connote the interaction of two variables: probability of failure (P_f) and the effect or consequence of that failure (C_f) as associated with the three interrelated attributes of technical performance, cost and schedule. P_f is the lack of success or an expression of the unreliability of the system, subsystem, configuration item, component or part. $P_f = 1 - P_s$, where P_s is the probability of success or an expression of the reliability of the element. $P_f + P_s = 1$.

The consequence of failure (C_f) is an expression of the non-utility of the element if it is unreliable. $C_f = 1 – C_s$, where C_s is the consequence of success or the utility of the element. $C_f + C_s = 1$.

Now a risk factor (RF) can be defined in terms of P_f and C_f, as follows:

RF = Risk Factor

= 1 - expected outcome

$= 1 - (P_s)(C_s)$

$= 1 - (1 - P_f)(1 - C_f)$

$= P_f + C_f - (P_f)(C_f)$

This RF is the union of the sets P_f and C_f. If P_f and C_f are mutually independent, their joint probability $(P_f)(C_f) = 0$ and RF = $P_f + C_f$. This occurs only when there is no consequence of failure ($C_f = 0$) and RF = P_f.

The job now becomes one of identifying the factors for determination of P_f and C_f. Various approaches may be used involving elements of P_f and C_f that may be derived from formulas, subjective assessments by panels of experts, or combinations thereof. For example, the value of P_f might be obtained by averaging values for five different attribute factors, as follows:

$P_f = (P_1 + P_2 + P_3 + P_4 + P_5)/5$, where:

P_1 = probability of failure due to degree of hardware maturity

P_2 = probability of failure due to degree of software maturity

P_3 = probability of failure due to degree of hardware complexity

P_4 = probability of failure due to degree of software complexity

P_5 = probability of failure due to dependency on other factors

Also, C_f might be obtained by averaging values for three different attribute factors as follows:

$C_f = (C_1 + C_2 + C_3)/3$, where:

C_1 = consequence of failure due to technical factors

C_2 = consequence of failure due to cost impacts

C_3 = consequence of failure due to schedule impacts

The results of the quantitative assessments are most meaningful if these attributes are derived from a panel of technical, operational and management experts.

Following the calculation of the risk factors (RF values), they should be ranked in order to identify those of most concern. A simple approach is to select arbitrary values of RF for grouping the items into high, medium and low categories of risk. As an example, consider:

Risk Factor	Risk Level	Action
$RF \geq 0.7$	High	The IV&V Team would report items in this category to the appropriate SFA management. If tasked, the IV&V Team would develop a risk abatement plan and continue to review the items to manage the associated risks.
$0.3 < RF < 0.7$	Medium	The IV&V Team would report the items in this category to the appropriate SFA management. If tasked, the Team would develop a risk abatement plan and follow these risk items for impact.
$RF \leq 0.3$	Low	The IV&V Team would monitor activity in project reviews.

Appendix C

SYSTEM MODEL SPECIFIC CONTROLS

APPENDIX C. SYSTEM MODEL SPECIFIC CONTROLS

C.1 Single Sign-On

Scor e	ASSESSMENT REQUIREMENT	Quality Value	Weighted Score	Note
	The system has Single Sign-On (SSO) capabilities for all classes of users who need to access more than one system, based on user access rights.			
	The SSO system is able to integrate with current SFA system security functionality.			
	The SSO product is able to interface with existing application, database, or network security by way of standard security interfaces. This will ensure that the SSO product will integrate with currently installed security products.			
	The SSO product provides the ability to enforce security rules enterprise-wide regardless of system platform. This will ensure consistent security over resources on all protected platforms.			
	All changes, modifications, additions, and deletions related to SSO are logged. This ensures that all security changes are recorded for review at a later time.			
	The SSO system enables the administrator to trace access to systems regardless of system or platform.			
	The SSO system provides for the administration of the product from any of the supported platforms. This enables the administrator to support the product from any platform.			
	All SSO mechanism related changes are made on-line/real-time. The ability to batch SSO related changes together is also important to enable easy loading or changing of large numbers of security resources or users.			
	The SSO system synchronizes security data across all entities and all platforms. This ensures that all security decisions are made with current security information.			
	The SSO product features a common control language across all serviced platforms so that system administrators do not have to learn different commands on different platforms.			

Score	ASSESSMENT REQUIREMENT	Quality Value	Weighted Score	Note
	The SSO product has the ability to restrict or control access on the basis of a terminal, node, or network address.			
	All releases of the SSO product are backward compatible or release independent. Features of new releases should co-exist with current features and not require a total reinstallation of the product. This ensures that the time and effort previously invested in the prior release of the product is not lost when a new release is installed.			
	The SSO product supports a phased implementation to enable administrators to implement the product on individual platforms without impacting other platforms. This will enable installation on a platform-by-platform basis if desired.			
	The SSO product includes a test facility to enable administrators to test security changes before placing them into production.			
	Security administration of the system is possible from a single point. This enables an administrator to provide support for the product from any device.			
	The SSO system can support the creation of spans of control so that administrators can be excluded from or included in certain security control areas within the overall security setup. This enables an administrator to decentralize the administration of security functions based on the groups/nodes/domains/enterprises over which the decentralized administrator has control.			

C.2 Encryption and Public Key Infrastructure (PKI)

Score	ASSESSMENT REQUIREMENT	Quality Value	Weighted Score	Note
	The strength of the algorithm used depends on the sensitivity of the resource or information being protected.			
	The algorithms undergo review in case of possible threats, reduction in the security provided through their use, taking into account newly available technology, or mathematical weakness of the encryption algorithm.			

Scor e	ASSESSMENT REQUIREMENT	Quality Value	Weighted Score	Note
	All encryption keys have an agreed upon limited usage. The same encryption key is used for only a specified number of times or for a specified period of time.			
	The system uses an algorithm with at least the strength of Triple DES, as required in the Draft FIPS PUB 46-3.			
	The PKI technology is interoperable and extensible, making sure that SFA can take advantage of later marketplace changes and improvements.			
	The technology is flexible, adaptable, extensible (able to serve users having divergent environments and interests), expandable, scalable (able to support a much larger user base), and interoperable.			
	The PKI meets Minimum Interoperability Specification for PKI Components (MISPC).			
	The PKI itself is secure.			
	The PKI protects the confidentiality, integrity and availability of the PKI services, for example key generation, key distribution, and key storage.			
	The PKI provides strong non-repudiation services for actions of certificate services.			
	The PKI prevents PKI services themselves from repudiating their own actions.			
	The PKI prevents users and subscribers from repudiating their own actions.			
	The system uses the services of a trusted certificate authority to manage the distribution of public keys.			
	Each key holder is identified uniquely, possibly by the public key itself.			
	There is a specified procedure for confirming the identity of a certificate holder (identity proofing).			
	The identity proofing mechanism supports proofs of identity that can be linked to legacy databases to verify the existence of the individual user.			
	The identity proofing mechanism incorporates methods to verify that the identity being "proofed" belongs to the individual requesting the certificate.			
	The identity proofing mechanism cross verifies the set of data elements as part of the verification process.			
	It is possible to ensure that only key recovery enabled systems shall be usable within a PKI implementation, where this is required.			

Scor e	ASSESSMENT REQUIREMENT	Quality Value	Weighted Score	Note
	The PKI specifies key recovery functionality for use in environments that require such functionality.			
	There is a specific policy for the protection and recovery of keys. The policy defines how the keys are to be protected and under what conditions and to whom a key will be made available.			
	The key recovery policy complies with federal standards and legislation.			
	The key recovery facility is unconditionally trusted and is liable to uphold the stated policy with redress for loss arising from failures to uphold policy through contractual liability and penalties.			
	A key recovery center is able to verify the legitimacy of a key submitted to it for storage.			
	A user of a key recovery repository is able to verify that it is an authorized repository.			
	The PKI provides for coordination between the management of public and private keys in PKI and in data recovery centers.			
	The PKI supports aging, revocation, and repudiation of keys.			
	The PKI supports discretionary key fragmentation between key recovery facilities.			
	The PKI supports facilities for the distribution of keys to appropriate storage devices and directories.			
	The PKI provides the certification authority with the capability to revoke certificates for individual keys under the terms of the applicable policy.			
	The PKI provides the certification authority with the ability to suspend and reactivate certificates for individual keys under the terms of the applicable policy.			
	The PKI provides the certification authority the capability to force delivery of revocation, suspension, and reactivation notices.			
	The PKI supports facilities to enable a user to repudiate his public key under the terms of the applicable policy.			
	The PKI supports facilities to enable a user to suspend and reactivate his public key under the terms of the applicable policy.			
	The PKI supports facilities to enable the user and subscriber to retrieve revocation, suspension, and reactivation notices.			

Scor e	ASSESSMENT REQUIREMENT	Quality Value	Weighted Score	Note
	The PKI supports facilities to enable the user and subscriber to determine the status (e.g., revoked or suspended) of a specific certificate.			
	The PKI supports facilities to enable the archive and subsequent retrieval of certificates in support of the retrieval and verification of long-term information in accordance with governance policy.			
	The PKI supports implementations that enable warranted law enforcement retrieval, subject to security policy and authorization compliance and approval.			
	The PKI supports implementations that enable warranted corporate agency retrieval, subject to policy and authorization compliance and approval.			
	The PKI supports implementations that enable warranted individual retrieval, subject to policy and authorization compliance and approval,			
	The PKI supports an electronic vehicle for the delivery of a notarized electronic warrant, to support the automation of key retrieval under due process (to take advantage of existing legal agreements)			
	For supporting warranted retrieval, a permanent, non-repudiable and independently verifiable record of encryption key retrieval operations is maintained.			
	The PKI provides distributed certificate management functionality.			
	PKI implementation supports policing and policy enforcement (PKI governance model).			
	Certification of the binding between a public key and a directory name is mandatory.			
	Certification of the binding between additional attributes and a directory name is discretionary.			
	Auditing and support for the monitoring of policy compliance is required.			
	The PKI implementation should provide concurrent support for multiple security policies.			
	The PKI implementation should provide support for exchange of digital certificates.			
	The PKI implementation should provide support for continuance of service in the event of transfer of certificate services from one certification authority to another.			

Scor e	ASSESSMENT REQUIREMENT	Quality Value	Weighted Score	Note
	The PKI implementation should provide support for arbitration to determine acceptability of certificates in the event of multiple conflicting certification paths.			

C.3 Directory Services

Scor e	ASSESSMENT REQUIREMENT	Quality Value	Weighted Score	Note
	Directory Services are based on globally accepted standards, so as to easily integrate with applications from most vendors.			
	The Directory shall provide a unified interface to the user, regardless of the physical location of the information accessed, and it shall possesses the necessary information to locate requested information, regardless of where the information might be on the network.			
	The Directory provides a strong authentication service for access.			
	There is Interoperability between Directory components.			
	The Directory shall integrate with the entire SFA security infrastructure.			
	The Directory is able to serve as a Digital Certificate Repository and interact with the PKI.			

C.4 Electronic Mail (Email)

Scor e	ASSESSMENT REQUIREMENT	Quality Value	Weighted Score	Note
	Electronic mail services use an appropriate Email encryption technology to authenticate messages.			
	Security sensitive electronic mail messages use a commonly accepted Email security standard such as S/MIME or PGP/MIME.			

C.5 Electronic Data Interchange (EDI)

Scor e	ASSESSMENT REQUIREMENT	Quality Value	Weighted Score	Note
	EDI security is based on widely accepted industry standards.			

Scor e	ASSESSMENT REQUIREMENT	Quality Value	Weighted Score	Note
	EDI security standards shall comply with FIPS PUB 161-1.			
	All EDI systems that are sensitive are identified (in compliance with the Computer Security Act of 1987).			
	There is a specific security plan for sensitive EDI systems.			
	Security training is conducted for personnel involved in the development and operation of EDI systems.			
	As with the rest of the systems, resources are allocated according to the risk and magnitude of potential harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained or transmitted by the EDI system.			
	There is a specified procedure for message repudiation.			
	Written agreements with interchange partners shall establish the specific security and authentication mechanisms to be used, and the legal acceptability, to the recipient, of the originator's electronic messages.			
	Message Integrity is ensured for all interchange of data.			
	Mechanisms to ensure confidentiality of EDI messages are employed.			
	Originator authentication is ensured for all EDI messages.			
	Non-Repudiation of parties involved in an exchange is ensured for all EDI transactions.			
	Contingency plans are implemented for all critical EDI infrastructure components in case of system failure or degradation.			
	Complete records of EDI interchanges are maintained.			
	Unauthorized modifications or alterations to records are prevented.			
	Modifications or alterations are automatically recorded in an electronic audit trail, including precise dates and times.			
	An electronic copy of each transmitted EDI message, together with the proof of approval, are retained for audit purposes as the audit trail.			

C.6 Databases

Scor e	ASSESSMENT REQUIREMENT	Quality Value	Weighted Score	Note
	The Database security environment is able to integrate with the enterprise wide security environment			
	The Database security environment is able to integrate with the Application security environments of all the applications that use it.			
	Controls over DBMS resources are adequately documented and implemented.			
	The DBMS has user groups set up corresponding to the user classes defined for the system.			
	User rights or permissions access are reviewed whenever changes are made to the system or user account.			
	User views of data corresponding to each user group are implemented, e.g., through a data dictionary.			
	There are access controls within the DBMS to protect the data dictionary security profiles.			
	There are appropriate access controls over the archive and backup copies of both the DBMS data and the DBMS configuration parameters.			
	There are screening procedures that ensure consistent security rules are applied to all DBMS and data dictionary data items regardless of the access path taken by a user.			
	There are appropriate access controls over DBMS internal user and resource profiles.			
	There are appropriate controls over access to and definition of data held within the DBMS, including: (1) schema definitions for physical database(s) used in hierarchical and network DBMS architecture (2) sub-schema definitions for logical views of data held within the DBMS (3) table definitions and the assignment of table authorities or views for relational databases, and (4) binding authorities (relational architectures).			

Scor e	ASSESSMENT REQUIREMENT	Quality Value	Weighted Score	Note
	There are adequate controls to monitor and maintain the integrity of the DBMS, including: (1) the use of referential integrity functions where these are available, (2) prevention of illogical deletion of database records, (3) check pointing to aid forward recovery, (4) controls within the DBMS or application level code to prevent mutual lockout of database records ("the deadly embrace"), (5) pointer creeping and index verification monitoring to verify data relationships, and (6) database synchronization across distributed or linked database components.			